Корінь Д. К., курсант 2-го курсу
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
*(Дніпропетровський державний
університет внутрішніх справ)*

ПРОБЛЕМИ ІНФОРМАЦІЙНОГО ЗАХИСТУ ПІДПРИЄМСТВ ТА УСТАНОВ

Вже досить довго багато компаній аналізують безпеку різних підприємств. Встановлюють різні структурні моделі комерційних підприємств, фінансових установ, банків, державних установ, навчальних закладів та слабозахищених, але важливих підприємств, державного значення. Фахівці з різних країн почали моделювати та організовувати хакерські напади на важливі об'єкти для подальшого аналізу збитків та системи безпеки. Протягом тривалого часу, приблизно 10 років, різні організації вивчали вплив багатьох факторів на розвиток загроз у кіберпросторі. Всі ці спроби фінансувалися окремими компаніями, які розробляють первісну частину захисту мережі, та державами, які використовують багато ресурсів для створення систем моніторингу, контролю та перевірки безпеки на державному рівні на основі певних стандартів. Найбільшу роль у розвитку таких систем відіграли США та Китай. Згідно з Вікіпедією, Департамент національної кібербезпеки (NCSD) є підрозділом управління кібербезпеки та комунікацій Директорату національної безпеки і програм, МВС США. Він був створений 6 червня 2003 року на базі Національного центру захисту інфраструктури, Федерального центру комп'ютерних інцидентів та Національної системи зв'язку. Місія NCSD полягає у співпраці з приватним сектором, урядом, військовими та розвідувальними органами для оцінки ризиків і зниження можливостей атакувати та загрожувати сфері інформаційних технологій та пристроїв, що мають безпосередній вплив на функціонування важливих IT-структур уряду США та приватного сектора. NCSD також надає аналіз системи внутрішньої та зовнішньої інформаційної безпеки, здійснює раннє попередження та допомогу, у разі надзвичайних ситуацій для державного та приватного секторів. Як частина всеосяжного національного плану для забезпечення кібербезпеки держави NCSD виконує більшість завдань міністерства. Бюджет NCSD на 2011 фінансовий рік становить 378 мільйонів доларів США. В Китаї інформація щодо державних технологій та розробок у межах кіберпростору є таємною та не оприлюднюється владою,

але в інтернеті можно знайти деяку інформацію щодо цього. За словами американського аналітика Джеймса Малвенона, організація військових кібероперацій Китаю прихована і децентралізована, а операції реалізуються за допомогою постійного мінливого складу офіційних, громадських та напівцивільних груп [1].

Принаймні з 2004 року у Народно-визвольній армії Китаю є підрозділ «61398», призначений для взлому та хакерських атак на комп'ютерні мережі противника. Окрім спеціальних сил Народно-визвольної армії, керівництво Китаю також використовує хакерські групи для проведення кібершпигунства та кібератак, наймасштабнішою з яких є «Альянс Червоних Хакерів» (Red Hacker Alliance), який, за деякими оцінками, налічує приблизно 80 тисяч осіб. За словами російських експертів з інформаційної безпеки В. С. Овчинського та Е. Ларіни, «Альянс Червоних Хакерів» – це неформальна, але контрольована урядом мережа, до складу якої входять не лише хакери з самого Китаю, а й громадяни Китаю з усього світу, які тісно співдіють з 3 та 4 управліннями Генерального штабу армії КНР [2].

Ці дані тривалий час зберігалися в таємниці і не розкривалися, не використовувалися в країні або щодо об'єктів, які становили чи могли становити загрозу. У кіберпросторі набагато складніше знайти об'єкти загрози, техніки та способи маскування, а також інструменти та засоби для влаштування хакерських атак. Саме це було причиною того, що багато підприємств та організацій не знали, що їх ресурси використовувалися для реалізації загроз: «рекламних вірусів», «хробаків», «вірусів-маскувальників». З роками хакери стали більш винахідливим та почали створювати віруси, які дуже швидко потрапляють у систему, ігноруючи будь-які перешкоди. Наприклад, зловмисники почали використовувати «віруси-маскувальтники» у вигляді важливого листа від родичів, керівництва на роботі або важливих повідомлень від постачальників програмного забезпечення. З аналізу вірусів, що становлять загрозу, 94 % з них використовуються для операційних систем Windows, приблизно 5 % – для операційних систем: MacOs, Unix, Linux та операційних систем приладів для комунікації та лише 1 % для авторських програмних забезпечень, які створені за власними розробками, де не враховані досвід та способи захисту від можливих загроз.

Сьогодні існує багато дискусій щодо питання побудови системи безпеки, але для вирішення цього питання, насамперед, треба розуміти, що для цього потрібен досвід та знання різних систем безпеки та протидії. Треба зазначити, що саме працівники, адміністратори та менеджери створюють систему безпеки на підприємстві або проводять комплексний аудит компанії, встановлюють заходи безпеки, організовують та встановлюють нагляд за інформативним середовищем компанії, але на їх шляху є багато проблем, які важко пояснити керівництву. Візьмемо, наприклад, попередні масштабні організації різних

форм власності. Коли віртуальне середовище та комп'ютерна інфраструктура не були розвинені, вони організували секретні підрозділи для контролю за витоком інформації та співпрацювали з СБУ, МВС та Міжнародною організацією кримінальної поліції.

В Україні політика кібербезпеки та інформаційного захисту покладена на численні державні органи, а саме: Державне агентство спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство внутрішніх справ України, Генеральний штаб України, Збройні сили України та навіть Національний банк України. Кожна з цих служб має свою галузь у сфері кібербезпеки, за якою встановлює контроль та несе відповідальність. За даними департаменту кіберполіції, кількість кіберзлочинів в Україні зросла в середньому на 2500 на рік. Згідно з доповіддю, опублікованою на вебсайті правоохоронних органів, співробітники кіберполіції брали участь у розслідуванні понад 10 тисяч встановлених кримінальних справ щодо високих технологій та IT-сфери. Загалом цього вистачало протягом довгого часу, але сьогодні кордони відкриті, і багато держав створили органи контролю за небезпечною діяльністю у кіберпросторі. У багатьох країнах ці агентства призначені для виявлення негативних активностей трафіку (спаму), обмеження доступу населенню до небезпечних секторів у мережі, встановлення засобів захисту державної та особистої інформації населення, а також заборони використання небезпечних чи заборонених урядом ресурсів.

Через високу вартість підтримки локальних серверів, модернізації, забезпечення баз даних, утримування IT-фахівців відповідного рівня, приватні компанії рідко використовують локальні сервери, замість цього підприємства можуть використовувати хмарні технології та підтримувати правильну організацію потоків інформації – це б дозволяло зекономити купу грошей та безпечно ресурс компанії. Важливим організаційним фактором захисту клієнтів є обізнаність працівників та дотримання ними основних правил використання робочого майна. На нашу думку, було б правильно заборонити працівникам компанії користуватися корпоративною поштою для приватного листування, зберігати та проводити обмін інформації за допомогою флеш-накопичувачів, по-перше, флеш-накопичувачі дуже уразливі для вірусів, по-друге, робоча інформація або інші ресурси – це власність компанії, а не інформація для розповсюдження, а за допомогою флеш-накопичувачів дуже легко її викрасти або копіювати стороннім особам. Також ми б рекомендували користуватися тільки ліцензованим антивірусом, який пройшов перевірку часом та організація, яка його створила, довела його ефективність. Вважаємо, що важливу роль також відіграє підготовленість та постійне підвищення професійного рівня працівників, саме тому рекомендуємо надати змогу фахівцям IT-сфери, юристам та бухгалтерам користуватися новими технологіями та проходити навчальні курси для отримання практичних навичок, підвищення кваліфікації.

Бібліографічні посилання

1. Національне управління кібербезпеки США. URL: uk.wikipedia.org/wiki/ Національне_управління_кібербезпеки_США.
2. Альянс червоних хакерів. URL: uk.wikipedia.org/wiki/Альянс_червоних_хакерів.

Костюк Ю. А., курсант 3-го курсу факультету підготовки фахівців для підрозділів стратегічних розслідувань
Науковий керівник – Неклеса О. В.,
викладач кафедри фінансових та стратегічних розслідувань
(Дніпропетровський державний університет внутрішніх справ)

СТРУКТУРА Й ОСОБЛИВОСТІ ЕКОНОМІЧНОЇ ЗЛОЧИННОСТІ НА СПОЖИВЧОМУ РИНКУ

На сьогодні Україна – одна з провідних держав з потужним зовнішньоекономічним потенціалом. Але з погляду найважливішого завдання – забезпечення якості життя і добробуту людей – до необхідного рівня ще далеко. Фундаментальним чинником, що зумовлює необхідність прийняття відповідних заходів, є падіння попиту домашніх господарств. На цей час це основний драйвер уповільнення виходу країни з кризи. У нинішній кризі два основних чинники: населення і торгова галузь.

Розвинути внутрішній ринок можна шляхом стимулювання попиту домашніх господарств через зростання доходів працюючих громадян і пенсіонерів, а попит з боку держави – через пом'якшення контрольно-наглядової діяльності і зростання кількості держзамовлень для малого і середнього бізнесу. Наявність такого феномена «працюючих бідних» не тільки обмежує купівельну спроможність великої частини населення, без якої розвиток внутрішнього ринку неможливий, але й підвищує соціальну напруженість. Крім того, це відбивається на продуктивності і якості праці, призводить до дефіциту кадрів у виробничій сфері.

Споживчий ринок є одним з найважливіших ланок всього ринкового механізму. Специфіка кожного елемента споживчого ринку визначається конкретними характеристиками і динамікою взаємодії між собою з метою забезпечення потреб населення і успішного функціонування економіки. Водночас споживчий ринок схильний не тільки до соціальних, економічних і політичних потрясінь, але також стикається з неринковим впливом кримінальних структур і тіньових економічних явищ. Поєднання цих чинників призводить до зростання частки «Живуть за межею бідності», до